Brief, only the Examiner's response to those arguments will be addressed in this brief.

A. Claim 1 is not Anticipated by Carter

Claim 1 provides, *inter alia*, for solving an access formula describing a function of groups. The Examiner admits that no such formula is taught by Carter.

> Carter does not explicitly disclose the feature of an access formula. However, this feature is deemed to be inherent to the Carter method because the entered password would have to be compared with a stored value in order to determine granting user access (see column 16, lines 16-29; figure 4, item 90; figure 9, step 152). The Carter method would be inoperative if such a comparison were not made.
>
> Examiner's Answer, pp. 4-5.

Assuming that the Examiner's characterization of Carter is correct, the issue can be stated as follows: Does matching an entered password with a stored password inherently teach an access formula describing a combination of groups?

The access formula is discussed with regards to Appellant's Figure 4 on page 15, lines 11-17, as follows:

> Access formula 102, also known as an access control list or ACL, expresses a logical combination of groups 82 and clients 22 for which access to encrypted information 96 will be granted. Solution of access formula 102 indicates that consumer client 44 is either specified as client 22 directly granted to access encrypted information 96 in access formula 102 or is a member of group 82 granted access to encrypted information 96 by access formula 102.

In one embodiment of Appellant's invention, a single user can satisfy the access formula. In another embodiment, the user may be a member of a group granted access to encrypted information. Yet another embodiment of an access formula is disclosed on page 10, lines 10-25, as follows:

> Another design challenge is the ability to permit access to information based on combinations of groups of clients 22. A group may be defined as those clients 22 which share a common mandate. For example, possible groups may be all members of

> the financial department, members of the Board of Directors, software engineers assigned to project X, and the like. It is desirable to permit access to information based on combinations of groups such as, for example, clients which are either members of the Board of Directors or are members of both project X and are senior software engineers. Another useful form of description is to permit access to any client which is a member of M-of-N groups. For example, a client 22 may be granted access if it is a member of any two-of-three groups, Group 1, Group 2, and Group 3. It will be recognized that one of ordinary skill in the art can express access to information as a boolean combination of groups. A group asserts true in the boolean combination when consumer client 44 which is a member of the group requests access to the information set protected by the access formula. Consumer client 44 may then be granted access to the information if the access formula resultant is true.

In this embodiment, the access formula describes a function of groups. The specification discloses that any of these embodiments, as well as others, may be combined into a single access formula. *See*, access formula example on pages 16-17.

In attempting to provide support that Carter inherently teaches the provision of claim 1 that the access formula describe a function of groups, the Examiner cites to Carter's key-seeking and member-seeking operations.

> After it has been determined that the document 54 to which access is requested is a work group document 90, the obtaining step 152 is performed by the collaborative access controller 44. As with other portions of the collaborative access controller 44, the portion which performs the obtaining step 152 may be embodied within the application 52 or may be a separate module which is invoked by the application 52 or by the user. The obtaining step 152 comprises interactively asking the user for its user identifier and a corresponding password. In alternative embodiments, the user identifier identifies the current user and is obtained by querying the operating system 46 or the object database system 62; only the password is obtained interactively from the user.
>
> Col. 16, ll. 16-29.

> If the key-seeking step 154 succeeds, a member-seeking step 158 is performed. The step 158 searches the member definitions 96 of the collaborative document 90 in an attempt to locate a member identifier 98 that corresponds to the user identifier obtained during the step 152. The search is accomplished substantially as described above in connection with the steps 122, 140, 142. If the search fails, then the user identifier does not identify a member of the collaborative group and the limiting step 156 is performed.
> If the search succeeds, a key-decrypting step 160 is performed.
> Col. 16, ll. 51-62.

The Examiner argues that Carter's searches, which appear to do nothing more than a password check followed by a group membership check, teach Appellant's claim limitation:

> It is clear that this search would require comparison to see that the member identifier, relating the member to the workgroup, is equal to the user identifier entered by the user to decrypt the document key and decrypt the document. This is within the scope of "solving an access formula describing a function of groups, each group comprising a list of at least one client, wherein the requesting consumer client is granted access to the information if the requesting consumer client is a member of at least one group which correctly solves the access formula" explicitly recited in claim 1. This matching comparison is within the scope of an access formula as described by the appellant in the specification (see specification, page 10, lines 10-25 and Figure 1, items 22 and 44). *In Carter, the client is a member of M-of-N groups, where both M and N equal one.*
>
> Examiner's Answer, pp. 15-16 (emphasis added).

However, if M=N=1, the access formula would be a function of only one *group*. Group is singular. The Examiner goes on to state that "Carter does not teach more complex formulas than a comparison ..." (Examiner's Answer, pg. 16.) Claim 1 provides that the access formula describes a function of *groups*. Groups is plural. Carter does not contemplate basing access on a function, or on more than one group, or on a function of such groups. The Examiner has impermissibly written the limitation "function of groups" out of claim 1.

B. Claim 9 is not Anticipated by Carter

Claim 9 provides, *inter alia*, for a key manager, at least one group server and at least one producer client. The key manager generates private key and public key matched pairs. Each group server maintains at least one group. Each group includes a list of client members allowed access to information produced by any client member of the group. Each group server also obtains a private key and matched public key *for each group*. Each producer client can encrypt an encryption value, used to encrypt an information set, with the an access formula and the public key *for each group* for which access to the information set may be granted.

The Examiner asserts that Carter teaches claim 9. Carter teaches obtaining a public key and a private key only for each authorized *user*, not each group. For example, column 13, line 63-column 14, line 5, is as follows (emphasis added):

> The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the *public key of the member in question.*, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, *but the encrypted form 100 of the document key is unique to each member*. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key.

Carter's "underlying document key" is roughly analogous to Appellant's encryption value. Carter teaches encrypting the document key with the public key of each authorized user (group member). The collection of group members and encrypted document keys are stored in a prefix associated with the encrypted information. See, Figures 4 and 5; column 12, lines 9-47. Carter's scheme is precisely the scheme described as problematic in Appellant's Background Art section on page 3 of the application, lines 5-28, as follows:

> Another possible solution is to encrypt the information into a data set as above and to create a prefix associated with the data set that contains a listing of each client authorized to access the information contained in the data set. The public key for each

> client is used by a host to encrypt the key required to decrypt the data set. The encrypted data set key for each client to which access is granted is also stored in the prefix. Several difficulties arise with this technique. First, the association of a prefix with a data set implies that the prefix and data set should be placed together in long term storage. This means that the storage device holding the prefix must be accessed in order to change the listing of clients authorized to access the information. In the case of backup or archiving to, for example, magnet tape, the tape must be obtained and loaded before the access list can be modified. A second difficulty arises if a client is to be added to the list of authorized clients in the prefix once the prefix has been created. In order to add a client, the private key for an authorized client must be obtained, the data set encryption key decrypted using the private key, and the data set encryption key reencrypted using the public key of the new client. A first implementation option is to permit new clients to be added only by an existing client, restricting access control onto to existing clients. A second option is to have an authorized client surrender its private key, creating a potential breach in security. A third difficulty arises in projects where a group of clients may have to access thousands of information sets, such as with software development. Changing authorization may require accessing the prefix for each information set. A fourth difficulty arises in attempting to implement combinations of client groups, such as granting access to any client which is a member of a first group or a member of a second group.

Appellant's invention avoids associating an encrypted key for each user with the encrypted data protected by the key, as required by Carter. Instead, Appellant's invention uses a group server to hold a group keys and group associations.

In support of his argument that Carter teaches Appellant's group server, the Examiner states the following:

> As per claim 9, Carter teaches a group server containing a private key and matched public key for each group: Column 8, lines 60-67 (cited text omitted) Column 11, lines 55-67 (cited text omitted) Figure 3, items 74, 76 78. Carter points out that the public key pairs are associated with the groups, not just with individual members of the groups. As pointed out in the response to arguments for Group A, these keys are used in

> decrypting the symmetric key used to decrypt the workgroup document.
>
> Examiner's Answer, pp. 17-19.

All three of the citations refer to the ability of certain operating systems to generate encryption keys. These operating systems are functioning as key servers, and not as Appellant's group server. Further, the fact that Carter teaches the use of keys to decrypt a group document does not teach or imply Appellant's group server obtaining matched keys for each *group*. Carter teaches merely checking to see if an accepted user is a member of a group.

> After it has been determined that the document 54 to which access is requested is a work group document 90, the obtaining step 152 is performed by the collaborative access controller 44. ... The obtaining step 152 comprises interactively asking the user for its user identifier and a corresponding password.
> * * *
> During a key-seeking step 154, the collaborative access controller 44 attempts to use the information provided during the step 152 to obtain the private key 80 of the identified user.
> * * *
> If the key-seeking step 154 succeeds, a member-seeking step 158 is performed. The step 158 searches the member definitions 96 of the collaborative document 90 in an attempt to locate a member identifier 98 that corresponds to the user identifier obtained during the step 152. The search is accomplished substantially as described above in connection with the steps 122, 140, 142. If the search fails, then the user identifier does not identify a member of the collaborative group and the limiting step 156 is performed.
> If the search succeeds, a key-decrypting step 160 is performed.
>
> Col. 16, ll. 16-62.

In Carter, the private key (required to decrypt the document key) is retrieved based only on the particular user attempting to access the document. Further, the key is retrieved *before* any attempt is made to determine if the user is a member of the group allowed access to the document. *See*, Figure 9, "a flowchart for restricting access to ta collaboratively encrypted document." Column 7, lines 8-10. Carter does not teach, expressly or inherently, a group server obtaining matched keys for each *group*.

C. Claim 11 is Patentable over Carter

Claim 11, which depends from claim 9, provides a system for the secure handling of information wherein *the access formula is a boolean combination of groups*. The Examiner provides the following argument in support of the assertion that Carter teaches such an access formula:

> As per claim 11, Carter discloses that the search results in one of either of two alternatives, failure or success. This is equivalent to the Boolean results of true or false. This feature is inherent to the system of Carter. The system of Carter would not function if this logical consequence did not result. Column 16, lines 51-61.

A search of a list of group members is not an access formula. Further, there is simply no way that a single search group can be used to form a boolean combination of groups.

D. Claim 3 is Patentable Over Carter in View of Feistel

Claim 3 provides, for creating at least one group comprising a list of at least one consumer client; for acquiring a public key and a matched private key for each group; and for determining an access formula expressing logical combination of the at least one group for which access to the information set will be granted. Solution of the access formula indicates that a consumer client belonging to the solution group may access the encrypted information set. The Examiner asserts this portion of claim 3 is taught by Carter. As described above, Carter teaches associating keys with each user, not with each group.

Claim 3 also provides for encrypting an information set based on a randomly generated number and encrypting the randomly generated number using the access formula and the public key for each of the at least one group granted access to the information set. The Examiner points to no teaching or suggestion, in either Carter or Feistel, of such an encryption.

E. Claim 7 is Patentable Over Carter in View of Feistel

Claim 7, which depends from claim 3, provides that the access formula is a boolean combination of groups. The Examiner does not rely on Feistel for rejecting claim 7.

As provided above, Carter does not teach or suggest a boolean combination of groups for any purpose, let alone to define an access formula.

A petition for a one month extension of time together with a check for $110 accompanies this Reply Brief. No additional fee is believed to be due. However, any additional fee may be withdrawn from Deposit Account No. 19-4545. A duplicate of this notice is enclosed for this purpose.

Respectfully submitted,

JAMES P. HUGHES

By: _____
Mark D. Chuey, Ph.D.
Registration No. 42,415
Agent for Applicant

Date: May 14, 2003

BROOKS & KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075
Phone: 248-358-4400
Fax: 248-358-3351